Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15882
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Finite-Key Analysis of BB84 and B92 QKD with Discrete Phase Randomization and Koashi Bound

Brenendra Putra Oktaviansyah[1)*], T. Sutojo[2)], Muhamad Akrom[3)]
[1,2,3)]Department of Informatics Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia
[1)]111202315020@mhs.dinus.ac.id, [2)]tsutojo@dsn.dinus.ac.id, [3]m.akrom@dsn.dinus.ac.id

Submitted :Feb 2, 2026 | **Accepted** : Feb 22, 2026 | **Published** : April 2, 2026

Abstract: Quantum Key Distribution (QKD) enables theoretically secure key exchange based on fundamental quantum principles such as the no-cloning theorem and Heisenberg's uncertainty principle. However, practical implementations remain vulnerable to side-channel attacks caused by device imperfections, while many existing studies primarily analyze asymptotic security or isolated attack scenarios rather than realistic finite-key conditions. Unlike prior studies that focus on asymptotic or single-attack analyses, this work presents a comprehensive finite-key security evaluation of BB84 and B92 protocols under hybrid side-channel attacks using Discrete Phase Randomization (DPR) as a lightweight mitigation strategy and the Koashi bound for improved phase-error estimation in B92. Numerical simulations are performed using realistic system parameters with a finite-key size of 100 billion pulses across ten representative attack scenarios. The results show that applying DPR (M = 32) significantly suppresses phase-sensitive attack-induced errors, reducing the quantum bit error rate (QBER) from 11–50% to approximately 1.5–3.02%, thereby restoring practical secure key generation. B92 with the Koashi bound achieves secure transmission distance improvements from 181.6 km to 190.8 km without attacks and reaches 187.0 km under hybrid attacks with DPR, slightly exceeding BB84 in certain conditions. Peak secret key rates reach 0.1363 bit/pulse for BB84 and 0.0741 bit/pulse for B92. These findings demonstrate that non-orthogonal protocols can remain competitive under realistic finite-key constraints using practical mitigation techniques, although literature based induced QBER assumptions remain a limitation.

Keywords: BB84, B92, Discrete Phase Randomization, Finite-Key Analysis, Koashi Bound, QBER, Quantum Key Distribution, Side-Channel Attacks

INTRODUCTION

Quantum Key Distribution (QKD) enables the establishment of a shared secret key using quantum states governed by the principles of quantum mechanics. Fundamental properties such as the no-cloning theorem and Heisenberg's uncertainty principle ensure that any eavesdropping attempt introduces detectable disturbances, making QKD a promising future-proof cryptographic paradigm resistant to both classical and quantum computational attacks (Durr-E-Shahwar et al., 2024; Scholten et al., 2024; Singh et al., 2025).

Originally proposed as a theoretical concept, QKD has evolved into a deployable technology integrated into modern optical communication infrastructures. Advances in photon sources, detectors, and optical fiber integration have enabled long-distance implementations and metropolitan-scale deployments (Cao et al., 2022; Sharma, Agrawal, Bhatia, Prakash, & Mishra, 2021). Among various protocols, BB84 and B92 remain foundational frameworks widely used as benchmarks for evaluating both theoretical developments and experimental implementations (Thakur, Chouksey, Chopra, Sadotra, & Kumar, 2025).

Despite strong theoretical security guarantees, practical QKD systems face significant challenges due to implementation imperfections. Side-channel attacks exploit hardware vulnerabilities such as detector mismatches, electromagnetic leakage, and timing or wavelength manipulation, potentially degrading system performance and reducing secret key rates (Granados, Velasquez, Cajo, & Antonieta-Alvarez, 2025). Although approaches such as Measurement-Device-Independent QKD (MDI-QKD) and advanced network topologies have been proposed to

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

mitigate these issues, practical deployments still require efficient countermeasures that balance security and system complexity (Cao et al., 2022; Lizama-Perez & López-Romero, 2025; Yan et al., 2025).

In addition to side-channel threats, finite-key effects represent a critical limitation in realistic QKD scenarios. Unlike asymptotic analyses that assume infinite transmission lengths, practical systems operate with finite signal numbers, increasing uncertainty in parameter estimation and directly impacting achievable secret key rates and secure transmission distances (Aquina et al., 2025; Decker et al., 2025; Zapatero, Wang, & Curty, 2023). Consequently, incorporating finite-size analysis is essential for evaluating real-world performance and operational feasibility.

Recent studies have explored advanced optimization approaches, including quantum machine learning, to improve QKD parameter estimation and robustness. However, these methods often introduce additional system complexity and computational overhead. Therefore, lightweight mitigation strategies that maintain practical feasibility remain highly desirable for real-world deployment (Decker et al., 2025; Purohit & Vyas, 2025).

Among proposed mitigation techniques, Discrete Phase Randomization (DPR) has demonstrated potential in reducing vulnerabilities related to phase-sensitive attacks and photon-number splitting. Furthermore, security bounds based on quantum complementarity, such as the Koashi bound, enable improved phase-error estimation, particularly for non-orthogonal protocols like B92. These approaches offer opportunities to enhance secure transmission distances and key generation performance without requiring additional mechanisms such as decoy states (Decker et al., 2025; Koashi, 2009; Liu, Lawey, & Razavi, 2025).

Despite these advances, a systematic finite-key evaluation of the B92 protocol under multiple and hybrid side-channel attacks remains limited. Existing studies predominantly emphasize asymptotic analyses, single-attack scenarios, or BB84-centered evaluations, leaving a gap in understanding the realistic performance and competitiveness of non-orthogonal protocols under practical constraints. A comprehensive analysis integrating finite-key effects, lightweight mitigation techniques such as DPR, and refined phase-error estimation using the Koashi bound is therefore needed.

Based on this motivation, this study performs a comprehensive numerical evaluation and comparative performance analysis of BB84 and B92 protocols under finite-key constraints and diverse side-channel attack scenarios. The analysis incorporates Discrete Phase Randomization and applies the Koashi bound to B92 using realistic system parameters projected for 2025. The study aims to reassess the practical competitiveness of B92 relative to BB84 and evaluate the effectiveness of lightweight mitigation strategies in improving security performance for contemporary QKD systems.

LITERATURE REVIEW

Recent studies increasingly explore Quantum Key Distribution (QKD) as a promising solution for post quantum secure communication, with BB84 and B92 serving as fundamental reference protocols. (Kish, Pieprzyk, & Camtepe, 2025) provide a comprehensive overview of QKD development, describing the transition from theoretical constructs toward real world deployments in countries such as the United States, China, and Japan. Their work highlights the robustness of BB84, which relies on orthogonal state encoding to detect eavesdropping through observable quantum disturbances.

Several studies have focused on improving QKD performance under realistic operational conditions. (Decker et al., 2025) investigate QKD optimization using quantum machine learning approaches and demonstrate that enhanced phase error estimation using the Koashi bound significantly improves the performance of non-orthogonal protocols such as B92. However, their results also reveal that B92 remains more vulnerable to side-channel attacks when no additional mitigation strategy is applied, motivating the integration of lightweight countermeasures.

Discrete Phase Randomization (DPR) has emerged as an effective mitigation technique against phase related vulnerabilities. (Currás-Lorenzo, Wooltorton, & Razavi, 2021) demonstrate that fully discrete phase randomization can suppress phase information leakage proportionally to 1/M, enabling secure transmission over extended distances. Similarly, (Yan et al., 2025) apply DPR within measurement device independent QKD architectures, achieving low quantum bit error rates (QBER) below 2% even under hybrid attack scenarios. These studies collectively establish DPR as a practical and computationally efficient method for mitigating side-channel risks.

Beyond protocol level improvements, applied research has examined QKD deployment in practical systems. (Roosan, Khan, Nirzhor, & Hai, 2025) propose hybrid security architectures combining QKD with post quantum cryptography for telemedicine applications, identifying B92 as a cost efficient alternative but noting persistent vulnerabilities such as detector blinding attacks. (Zapatero, Navarrete, & Curty, 2025) further analyze implementation level threats, including detector mismatches and photon number splitting attacks, confirming that DPR can reduce QBER significantly in several scenarios.

Scalability and network integration also present challenges for practical deployment. (Lizama-Perez & López-Romero, 2025) introduce loop-back QKD network topologies incorporating DPR, but their findings indicate performance degradation in finite-key regimes due to limited signal statistics, consistent with earlier finite-key

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15882
e-ISSN : 2541-2019
p-ISSN : 2541-044X

studies (Curty et al., 2014). These results emphasize the necessity of evaluating QKD protocols under realistic finite-key constraints rather than relying solely on asymptotic assumptions.

From a comparative perspective, BB84 is generally considered more robust against side-channel attacks due to orthogonal state encoding, whereas B92 requires accurate phase error estimation to avoid overly conservative security bounds. The Koashi bound provides tighter estimation for non-orthogonal protocols and has been shown to improve B92 performance (Decker et al., 2025; Koashi, 2009). Nevertheless, existing studies often analyze DPR, finite-key effects, or protocol specific optimizations independently rather than within a unified framework.

Based on the reviewed studies, existing works predominantly focus on asymptotic regimes, single attack scenarios, or complex mitigation strategies requiring significant system overhead. A systematic finite-key evaluation of B92 under multiple and hybrid side-channel attacks remains limited. Addressing this gap, the present study integrates Discrete Phase Randomization and the Koashi bound into a unified finite-key analysis framework to systematically compare BB84 and B92 protocols under realistic attack conditions and reassess the practical competitiveness of non-orthogonal QKD protocols.

METHOD

Simulation Workflow and Reproducibility

This study uses a numerical simulation framework to evaluate the performance of the BB84 and B92 quantum key distribution (QKD) protocols under limited key constraints and multiple side-channel attack scenarios. All simulations are implemented in the Python programming language using the NumPy library for numerical computation. The QKD system is modeled over a single-mode fiber optic channel with transmission distances ranging from 0 to 200 km, uniformly sampled at 1001 discrete points, following a distance sweep approach similar to that of (Zapatero et al., 2023). For each distance point, the channel transmission is calculated using standard fiber loss assumptions, and the corresponding detection statistics are evaluated.

To ensure deterministic and reproducible results, a fixed random seed is used throughout the simulations. The total number of transmitted quantum signals is set to 100 billion to account for limited key effects. System parameters such as detector efficiency, intrinsic misalignment error, and background noise are kept constant across all scenarios unless otherwise stated. Side-channel attacks are introduced by setting the attack-induced error rate (QBER) adopted from the existing literature. These values are treated as assumed input parameters, and their mapping to the effective QBER after applying Discrete Phase Randomization (DPR) countermeasures is explicitly modeled. The effective QBER is then used to evaluate the secret key rate under a restricted-key security analysis.

For each transmission distance and attack scenario, the simulation computes the quantum bit error rate, estimates the phase error, and evaluates the corresponding restricted-key secret key rate for the BB84 and B92 protocols. The maximum secure transmission distance and optimal key generation rate are extracted from the resulting key rate curves. Step-by-step pseudocode describing the complete numerical procedure, including parameter initialization, distance sweeping, QBER calculation, DPR mitigation, and key rate evaluation, is provided to facilitate independent verification. The simulation framework was implemented in Python using a fixed random seed to ensure reproducibility. The implementation scripts supporting the findings of this study are available from the corresponding author upon reasonable request. A public repository will be released upon acceptance of the manuscript.

Research Stages

The workflow of the simulation-based research is illustrated in the figure below:

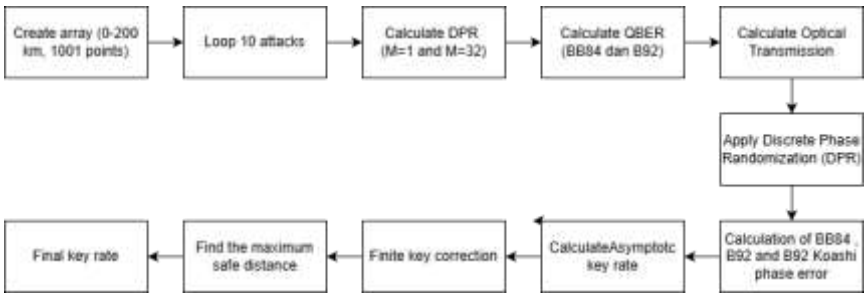

Figure 1 . Research Stage

System Parameters and Channel Model

The simulation parameters are selected to represent realistic conditions for QKD implementations projected for the year 2025. These parameters include the optical fiber attenuation coefficient ($\alpha = 0.20$ dB/km), detector efficiency ($\eta_{det} = 0.18$), dark count probability ($p_{dark} = 8 \times 10^{-8}$), misalignment error ($e_d = 0.015$), and error

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15882
e-ISSN : 2541-2019
p-ISSN : 2541-044X

correction inefficiency (f_ec = 1.16) based on a Low-Density Parity-Check (LDPC) coding scheme. In addition, a total number of transmitted pulses of N_total = 10^{11} is assumed for the finite-key analysis (Aquina et al., 2025; Decker et al., 2025; Zapatero et al., 2023).

Transmission through the quantum channel follows an exponential loss model. The channel transmittance as a function of transmission distance is expressed as(Cao et al., 2022; Zapatero et al., 2023):

$$\eta(d) = 10^{-\alpha d/10} \tag{1}$$

The total channel efficiency is then calculated as the product of the channel transmittance and the detector efficiency (Zapatero et al., 2023):

$$\eta_{\text{ch}} = \eta(d) \cdot \eta_{\text{det}} \tag{2}$$

For error correction and privacy amplification processes, the binary entropy function is employed to quantify the information leakage and correction overhead (Chen, Chen, & Yan, 2024):

$$h_2(x) = -x\log_2 x - (1-x)\log_2(1-x) \tag{3}$$

In addition, a Discrete Phase Randomization (DPR) mechanism is applied to reduce error rates induced by phase-based side-channel attacks, using a discrete number of phase states with M = 32 (Zapatero et al., 2023). The effective Quantum Bit Error Rate (QBER) after the application of DPR is determined by combining the intrinsic system error with the attack-induced error, scaled by the number of discrete phases:

$$E = e_d + \frac{E_{\text{eve}} - e_d}{M} \tag{4}$$

BB84 Protocol Model

For the BB84 protocol, the detection probability (gain) is defined based on the total channel efficiency and the detector dark count probability (Zapatero et al., 2023):

$$Q = \eta_{\text{ch}} + 2p_{\text{dark},} \tag{5}$$

The effective QBER is obtained from the combination of system imperfections and side-channel attack effects after applying DPR (Decker et al., 2025). The asymptotic secret key rate for the BB84 protocol is then calculated by accounting for error correction inefficiency and privacy amplification (Denys, Brown, & Leverrier, 2021):

$$r_\infty = Q[1 - f_{\text{ec}}h_2(E) - h_2(E)] \tag{6}$$

To incorporate finite-key effects, a security correction corresponding to a 7σ confidence level is applied (Curty et al., 2014; Hayashi & Tsurumaru, 2012):

$$\delta = 7\sqrt{\frac{Q}{\eta_{\text{ch}} N_{\text{total}}}} \tag{7}$$

The final secret key rate for BB84 is obtained by subtracting the finite-key correction term from the asymptotic key rate and enforcing non-negativity (Zapatero et al., 2023):

$$r = \max(0, r_\infty - \delta). \tag{8}$$

B92 Protocol Model

For the B92 protocol, the detection probability is defined similarly, but scaled according to the protocol's non-orthogonal state structure (Zapatero et al., 2023):

$$Q_\mu = \frac{\eta_{\text{ch}}}{2} + 2p_{\text{dark}} \tag{9}$$

The effective QBER is computed in the same manner as for the BB84 protocol, incorporating both system errors and side-channel attack contributions after DPR (Decker et al., 2025). The asymptotic secret key rate of the B92 protocol is given by (Koashi, 2009; Zapatero et al., 2023):

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15882
e-ISSN : 2541-2019
p-ISSN : 2541-044X

$$r_\infty = Q_\mu(1 - h_2(E)) \tag{10}$$

The information leakage due to error correction is calculated as (Koashi, 2009; Zapatero et al., 2023):

$$\text{leakage} = Q_\mu \cdot f_{\text{ec}} \cdot h_2(E) \tag{11}$$

Accordingly, the net secret key rate is expressed as (Curty et al., 2014; Zapatero et al., 2023):

$$r = r_\infty - \text{leakage} \tag{12}$$

To account for finite-key effects, a security correction with a confidence level of $7\sigma$is applied (Curty et al., 2014; Hayashi & Tsurumaru, 2012), defined as:

$$\delta = 7\sqrt{\frac{Q_\mu + 4p_{\text{dark}}}{\eta_{\text{ch}} N_{\text{total}}}} \tag{13}$$

Finally, the achievable secret key rate of the B92 protocol is obtained as (Zapatero et al., 2023):

$$r = \max(0, r - \delta) \tag{14}$$

B92 Protocol Model with Koashi Bound

In this approach, the phase error rate is estimated using the Koashi bound. The detection probability remains defined as in the standard B92 model, while the phase error is inferred from the observed QBER and the conditional detection probability (Decker et al., 2025; Koashi, 2009; Zapatero et al., 2023):

$$e_{\text{phase}} = E \cdot \frac{Q_\mu}{Q_c}, Q_c = \eta_{\text{ch}}(1 - e_d) \tag{15}$$

The asymptotic secret key rate is then computed by accounting for both the bit error rate and the estimated phase error (Koashi, 2009; Zapatero et al., 2023):

$$r_\infty = Q_\mu\left[1 - h_2(E) - h_2(e_{\text{phase}})\right] \tag{16}$$

For finite-key analysis under the Koashi bound framework, a security correction corresponding to a 5σ confidence level is applied (Curty et al., 2014; Hayashi & Tsurumaru, 2012):

$$\delta = 5\sqrt{\frac{Q_\mu}{\eta_{\text{ch}} N_{\text{total}}}} \tag{17}$$

The final secret key rate is obtained by subtracting this correction from the asymptotic key rate and enforcing non-negativity (Zapatero et al., 2023):

$$r = \max(0, r_\infty - \delta). \tag{18}$$

Side-Channel Attack Model and Secure Distance Calculation

The induced QBER values for the ten side-channel attacks are adopted as representative assumptions based on experimental reports and security reviews of practical QKD implementations. The attack types (time-shift, trojan-horse, wavelength, laser damage, faked-state, detector mismatch, electromagnetic leakage, photon-number splitting, hybrid, and blinding) are adopted from (Aquina et al., 2025; Decker et al., 2025; Zapatero et al., 2023), which discuss these vulnerabilities at the conceptual and implementation levels. The numerical QBER values are not directly taken from a single experimental dataset, but are assumed as realistic representative values consistent with ranges reported in practical QKD experiments and security analyses (Zapatero et al., 2023). These induced QBER values are selected as conservative upper bound assumptions to represent realistic worst case attack conditions, ensuring that the security evaluation does not rely on overly optimistic performance estimates.

The B92 protocol is assumed to exhibit higher vulnerability to certain attacks due to its use of non-orthogonal quantum states (Begimbayeva & Zhaxalykov, 2022). Higher QBER values are assigned to B92 to reflect its non-orthogonal signal structure and increased sensitivity to phase- and intensity-based leakage. A baseline system

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15882
e-ISSN : 2541-2019
p-ISSN : 2541-044X

misalignment error of 1.5% is assumed, following commonly adopted parameters for practical fiber based QKD systems (Pathak, Chaudhary, Sangeeta, & Kanseri, 2023). These values are mapped to the effective QBER after DPR mitigation using which suppresses phase sensitive attack-induced errors by a factor of 1/M, while detector blinding attacks remain unaffected due to their operation in the classical system (Decker et al., 2025; Zapatero et al., 2023). A detailed sensitivity analysis with respect to variations in the assumed QBER values is left for future work, as the present study focuses on comparative protocol evaluation under representative attack scenarios. The QBER value assumptions used for the BB84 and B92 simulations for each attack scenario are summarized in a separate table:

Table 1
Assumed Induced QBER Values for Simulated Side-Channel Attacks

Attack	BB84 QBER (%)	B92 QBER (%)
No Attack	1.50	1.50
Time-Shift Attack	33.00	45.00
Trojan-Horse Attack	11.50	40.00
Wavelength Attack	25.00	35.00
Laser Damage Attack	30.00	40.00
Faked-State Attack	20.00	30.00
Detector Mismatch Attack	28.00	38.00
Eelectromagnetic (EM) Leakage Attack	22.00	32.00
Photon-Number Splitting (PNS) Attack	35.00	45.00
Hybrid Attack	38.00	50.00
Blinding Attack	50.00	50.00

The maximum secure transmission distance is defined as the longest optical fiber distance at which the secret key rate remains positive and exceeds a practical threshold. Following common practice in QKD performance evaluation, this threshold is set to a secret key rate greater than 10^{-7} bits per pulse (Aquina et al., 2025; Cao et al., 2022; Zapatero et al., 2023):

$$d_{\max} = \max\{d \mid r(d) > 10^{-7}\} \tag{19}$$

This criterion is widely adopted to assess the feasibility of QKD systems under realistic deployment scenarios.

RESULT

The results obtained from the simulation process are summarized in tabular form, presenting the type of side-channel attack, applied mitigation technique, maximum secure transmission distance, resulting Quantum Bit Error Rate (QBER), and the maximum average secret key rate for the BB84 and B92 protocols. The results are organized following the logical flow of the research methodology and reflect the outcomes after applying the finite-key analysis and mitigation techniques described in the Methods section.

BB84 Protocol

The simulation results for the BB84 protocol are presented in Table 2. The table reports the performance of BB84 under various side-channel attack scenarios, including the corresponding QBER values, achievable maximum secure distances, and average secret key rates after applying Discrete Phase Randomization (DPR) and finite-key corrections.

Table 2
Result BB84 Protocol

Attack	M=1 Distance (km)	M=1 QBER (%)	Key Rate Max (bit/pulse)	M=32 Distance (km)	M=32 QBER (%)	Key Rate Max (bit/pulse)
No Attack	189.4 km	1.50	0.13629214	189.4 km	1.50	0.13629214
Time-Shift Attack	0 km	33.00	0	185.6 km	2.48	0.11472397

*name of corresponding author

Trojan-Horse Attack	0 km	11.50	0	188.2 km	1.81	0.12913094
Wavelength Attack	0 km	25.00	0	186.6 km	2.23	0.11994524
Laser Damage Attack	0 km	30.00	0	186.0 km	2.39	0.11666418
Faked-State Attack	0 km	20.00	0	187.2 km	2.08	0.12328905
Detector Mismatch Attack	0 km	28.00	0	186.2 km	2.33	0.11796935
Eelectromagnetic (EM) Leakage Attack	0 km	22.00	0	187.0 km	2.14	0.12194372
Photon-Number Splitting (PNS) Attack	0 km	35.00	0	185.4 km	2.55	0.11344184
Hybrid Attack	0 km	38.00	0	185.0 km	2.64	0.11153515
Blinding Attack	0 km	50.00	0	0 km	50.00	0

B92 Protocol

The corresponding results for the B92 protocol are summarized in Table 3. This table illustrates the impact of different side-channel attacks on the B92 protocol, highlighting the variations in QBER, secure transmission distance, and average secret key rate when finite-key effects are taken into account.

Table 3
Result B92 Protocol

Attack	M=1 Distance (km)	M=1 QBER (%)	Key Rate Max (bit/pulse)	M=32 Distance (km)	M=32 QBER (%)	Key Rate Max (bit/pulse)
No Attack	181.6 km	1.50	0.06814155	181.6 km	1.50	0.06814155
Time-Shift Attack	0 km	45.00	0	176.4 km	2.86	0.05357530
Trojan-Horse Attack	0 km	40.00	0	177.0 km	2.70	0.05513282
Wavelength Attack	0 km	35.00	0	177.6 km	2.55	0.05671639
Laser Damage Attack	0 km	40.00	0	177.0 km	2.70	0.05513282
Faked-State Attack	0 km	30.00	0	178.2 km	2.39	0.05832756
Detector Mismatch Attack	0 km	38.00	0	177.2 km	2.64	0.05576304
Eelectromagnetic (EM) Leakage Attack	0 km	32.00	0	178.0 km	2.45	0.05767967
Photon-Number Splitting (PNS) Attack	0 km	45.00	0	176.4 km	2.86	0.05357530
Hybrid Attack	0 km	50.00	0	175.8 km	3.02	0.05204245
Blinding Attack	0 km	50.00	0	0 km	50.00	0

B92 Protocol with Koashi Bound

The simulation outcomes for the B92 protocol incorporating the Koashi bound are presented in Table 4. The table reports the resulting QBER, maximum secure distance, and secret key rates obtained when phase error estimation is performed using the Koashi bound under finite-key conditions and side-channel attack scenarios.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15882
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Table 4
Result B92 Protocol with Koashi Bound

Attack	M=1 Distance (km)	M=1 QBER (%)	Key Rate Max (bit/pulse)	M=32 Distance (km)	M=32 QBER (%)	Key Rate Max (bit/pulse)
No Attack	190.8 km	1.50	0.07406923	190.8 km	1.50	0.07406923
Time-Shift Attack	0 km	45.00	0	187.4 km	2.86	0.06328516
Trojan-Horse Attack	0 km	40.00	0	187.8 km	2.70	0.06444353
Wavelength Attack	0 km	35.00	0	188.2 km	2.55	0.06561999
Laser Damage Attack	0 km	40.00	0	187.8 km	2.70	0.06444353
Faked-State Attack	0 km	30.00	0	188.6 km	2.39	0.06681564
Detector Mismatch Attack	0 km	38.00	0	188.0 km	2.64	0.06491188
Eelectromagnetic (EM) Leakage Attack	0 km	32.00	0	188.4 km	2.45	0.06633500
Photon-Number Splitting (PNS) Attack	0 km	45.00	0	187.4 km	2.86	0.06328516
Hybrid Attack	0 km	50.00	0	187.0 km	3.02	0.06214392
Blinding Attack	0 km	50.00	0	0 km	50.00	0

Comparative Analysis

To provide a comprehensive evaluation of protocol performance under realistic attack conditions, a comparative analysis between the BB84 and B92 protocols incorporating the Koashi bound is conducted based on the secret key rate as a function of transmission distance. This analysis aims to highlight the relative robustness of orthogonal and non-orthogonal encoding schemes under finite-key constraints and hybrid side-channel attacks.

Figure 2 illustrates the secret key rate versus transmission distance curves under the hybrid attack scenario for both protocols with and without Discrete Phase Randomization (DPR). The dashed horizontal line represents the practical security threshold of 10^{-7} bits per pulse, which defines the maximum secure transmission distance. The results show that the application of DPR (M=32) consistently improves performance by reducing the effective QBER, thereby extending the secure communication range for both protocols. While BB84 demonstrates higher robustness due to its orthogonal state encoding, the B92 protocol with the Koashi bound exhibits significant performance recovery compared to its standard formulation.

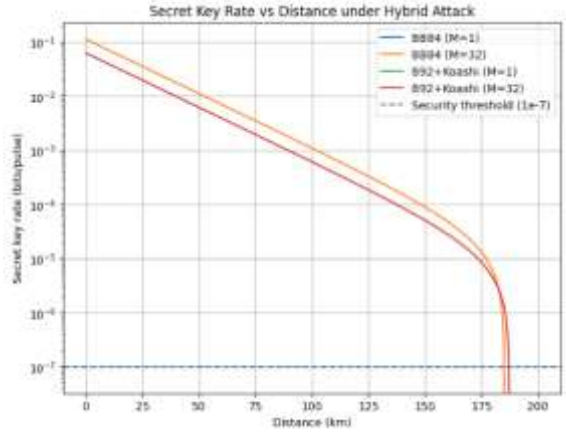

Figure 2 . Secret Key Rate vs Distance under Hybrid Attack

As observed, BB84 maintains a higher secret key rate across most transmission distances, particularly at shorter ranges where the gain remains relatively high. However, the performance gap between BB84 and B92 decreases

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15882
e-ISSN : 2541-2019
p-ISSN : 2541-044X

after incorporating the Koashi bound, indicating that refined phase error estimation can effectively mitigate the inherent disadvantages of non-orthogonal state encoding. This result supports the hypothesis that lightweight security enhancements can improve the practical viability of B92 without introducing substantial system complexity.

Figure 3 presents a focused comparison between BB84 and B92 and Koashi under DPR (M=32), emphasizing the influence of phase error estimation and mitigation techniques under identical attack conditions. The curves show that B92 with Koashi threshold achieves slightly longer secure transmission distances compared to BB84 under identical hybrid attack conditions. This result highlights the advantage of tighter phase error estimation in B92, while BB84 maintains a higher lock rate in the short to medium range regime..

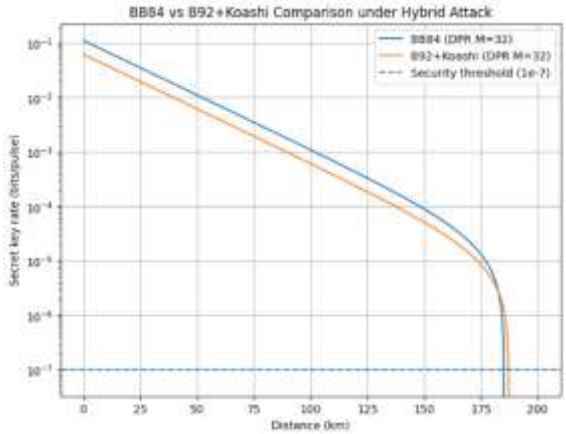

Figure 3 . BB84 vs B92 and Koashi Comparison

Overall, the comparative results demonstrate that combining Discrete Phase Randomization with the Koashi bound significantly enhances the resilience of B92 against hybrid side-channel attacks. These findings suggest that non-orthogonal protocols, when supported by appropriate finite-key analysis and lightweight mitigation strategies, can achieve performance levels approaching those of BB84 in realistic deployment scenarios.

DISCUSSIONS

This study makes three primary scientific contributions to the practical security evaluation of discrete variable QKD protocols under realistic finite-key conditions.

Finite-key reassessment of B92 under hybrid attacks

This work provides a finite-key security reassessment of the B92 protocol under a hybrid side-channel attack model that combines photon number related leakage and detector imperfections. Unlike conventional asymptotic analyses, the present study evaluates performance under finite statistical constraints, thereby offering a deployment oriented perspective. The results demonstrate that, although B92 is traditionally considered more vulnerable in high loss regimes, its performance can remain competitive when analyzed using refined phase error estimation and practical mitigation techniques. This reassessment clarifies the realistic security boundaries of B92 beyond idealized asymptotic assumptions.

Demonstration of Discrete Phase Randomization (DPR) as a lightweight mitigation strategy

The study quantitatively demonstrates that Discrete Phase Randomization with a moderate number of phase states (M = 32) is sufficient to significantly suppress phase based side-channel leakage. The results show substantial QBER reduction and secure distance restoration across multiple attack scenarios without requiring complex hardware modifications or decoy state implementation. These findings support DPR as a lightweight and practically implementable countermeasure, particularly suitable for resource constrained or simplified QKD deployments.

Quantitative comparison without decoy state techniques

The A controlled comparative evaluation between BB84 and B92 with and without the Koashi bound is performed without incorporating decoy state methods. This design isolates the intrinsic robustness of the encoding and phase error estimation mechanisms under identical attack assumptions. By avoiding decoy state enhancements, the analysis highlights the fundamental security performance trade offs of both protocols and demonstrates that

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

properly mitigated B92 can achieve performance comparable to BB84 in finite-key regimes. This contributes to a clearer understanding of protocol selection in simplified QKD architectures.

Collectively, these contributions strengthen the understanding of finite-key QKD security under hybrid attack models and provide practical insight into mitigation strategies that balance security enhancement with implementation complexity.

CONCLUSION

This study presents a systematic finite-key comparison between the BB84 and B92 QKD protocols under ten representative side-channel attack scenarios using projected realistic system parameters for 2025. By incorporating Discrete Phase Randomization (DPR) with M = 32 and applying the Koashi bound to B92, the work addresses the practical security and performance trade-offs of orthogonal and non-orthogonal encoding schemes in deployment-oriented conditions.

The results demonstrate that DPR effectively suppresses most phase based side-channel attacks, reducing the QBER from 11–50% to approximately 1.8–3.02% and restoring secure transmission distances to 175–188 km. The integration of the Koashi bound significantly improves B92 performance through tighter phase-error estimation, allowing B92 to achieve secure distances comparable to, and in several scenarios slightly exceeding, BB84. These findings reaffirm that non-orthogonal protocols remain viable when supported by refined finite-key analysis and lightweight mitigation strategies.

From a network design perspective, the results indicate that DPR enhanced protocols can provide robust metropolitan scale QKD links without requiring complex decoy state implementations. The demonstrated key rates of 136 Mbit/s for BB84 and 74 Mbit/s for B92 at a 1 Gbps repetition rate suggest suitability for high throughput real time applications, including secure video transmission and telemedicine, within trusted node network architectures. However, the persistence of detector blinding vulnerabilities underscores the importance of integrating detector independent countermeasures, such as measurement device independent QKD, in scenarios requiring full end to end security.

Practically, BB84 remains preferable in high loss or adversarial environments where maximal protocol maturity and widespread validation are prioritized. In contrast, B92 may be considered a competitive and cost effective alternative in resource constrained or hardware simplified deployments, particularly when decoy state techniques are not implemented and when DPR based mitigation is available.

Overall, this work demonstrates that the competitiveness of B92 should not be evaluated solely under asymptotic assumptions but rather within realistic finite-key and side-channel aware conditions. The findings contribute actionable insights for scalable QKD network design, balancing security robustness, implementation complexity, and cost efficiency.

REFERENCES

Aquina, N., Cimoli, B., Das, S., Hövelmanns, K., Weber, F. J., Okonkwo, C., … Verschoor, S. (2025). A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography. *EPJ Quantum Technology*, *12*(1). doi:10.1140/epjqt/s40507-025-00350-5

Begimbayeva, Y., & Zhaxalykov, T. (2022). Research of quantum key distribution protocols: BB84, B92, E91. *Scientific Journal of Astana IT University*, *10*, 4–14. doi:10.37943/QRKJ7456

Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., & Hanzo, L. (2022). The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet. *IEEE Communications Surveys and Tutorials*, *24*(2), 839–894. doi:10.1109/COMST.2022.3144219

Chen, L., Chen, X. M., & Yan, Y. L. (2024). Research on time-division multiplexing for error correction and privacy amplification in post-processing of quantum key distribution. *Scientific Reports*, *14*(1). doi:10.1038/s41598-024-77047-9

Currás-Lorenzo, G., Wooltorton, L., & Razavi, M. (2021). Twin-Field Quantum Key Distribution with Fully Discrete Phase Randomization. *Physical Review Applied*, *15*(1). doi:10.1103/PhysRevApplied.15.014016

Curty, M., Xu, F., Cui, W., Lim, C. C. W., Tamaki, K., & Lo, H. K. (2014). Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Communications*, *5*. doi:10.1038/ncomms4732

Decker, T., Gallezot, M., Kerstan, S. F., Paesano, A., Ginter, A., & Wormsbecher, W. (2025). Quantum key distribution as a quantum machine learning task. *Npj Quantum Information*, *11*(1). doi:10.1038/s41534-025-01088-9

Denys, A., Brown, P., & Leverrier, A. (2021). Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, *5*. doi:10.22331/Q-2021-09-13-540

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Durr-E-Shahwar, Imran, M., Altamimi, A. B., Khan, W., Hussain, S., & Alsaffar, M. (2024). Quantum Cryptography for Future Networks Security: A Systematic Review. *IEEE Access*, *12*, 180048–180078. doi:10.1109/ACCESS.2024.3504815

Granados, G., Velasquez, W., Cajo, R., & Antonieta-Alvarez, M. (2025). Quantum Key Distribution in Multiple Fiber Networks and Its Application in Urban Communications: A Comprehensive Review. *IEEE Access*, *13*, 100446–100461. doi:10.1109/ACCESS.2025.3577086

Hayashi, M., & Tsurumaru, T. (2012). Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths. *New Journal of Physics*, *14*. doi:10.1088/1367-2630/14/9/093014

Kish, S., Pieprzyk, J., & Camtepe, S. (2025). Quantum Key Distribution. Retrieved from http://arxiv.org/abs/2507.23192

Koashi, M. (2009). Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, *11*. doi:10.1088/1367-2630/11/4/045018

Liu, Z., Lawey, A., & Razavi, M. (2025). Analytical bounds for decoy-state quantum key distribution with discrete phase randomization. Retrieved from http://arxiv.org/abs/2508.14664

Lizama-Perez, L. A., & López-Romero, J. M. (2025). Loop-Back Quantum Key Distribution (QKD) for Secure and Scalable Multi-Node Quantum Networks. *Symmetry*, *17*(4). doi:10.3390/sym17040521

Pathak, N. K., Chaudhary, S., Sangeeta, & Kanseri, B. (2023). Phase encoded quantum key distribution up to 380 km in standard telecom grade fiber enabled by baseline error optimization. *Scientific Reports*, *13*(1). doi:10.1038/s41598-023-42445-y

Purohit, K., & Vyas, A. K. (2025). Quantum key distribution through quantum machine learning: a research review. *Frontiers in Quantum Science and Technology*, *4*. doi:10.3389/frqst.2025.1575498

Roosan, D., Khan, R., Nirzhor, S., & Hai, F. (2025). Post-Quantum Cryptography Resilience in Telehealth Using Quantum Key Distribution. *Blockchain in Healthcare Today*, *8*(1). doi:10.30953/bhty.v8.379

Scholten, T. L., Williams, C. J., Moody, D., Mosca, M., Hurley, W., Zeng, W. J., … Gambetta, J. M. (2024). Assessing the Benefits and Risks of Quantum Computers. Retrieved from http://arxiv.org/abs/2401.16317

Sharma, P., Agrawal, A., Bhatia, V., Prakash, S., & Mishra, A. K. (2021). Quantum Key Distribution Secured Optical Networks: A Survey. *IEEE Open Journal of the Communications Society*. Institute of Electrical and Electronics Engineers Inc. doi:10.1109/OJCOMS.2021.3106659

Singh, S. K., Kumar, S., Chhabra, A., Sharma, A., Arya, V., Srinivasan, M., & Gupta, B. B. (2025). Advancements in secure quantum communication and robust key distribution techniques for cybersecurity applications. *Cyber Security and Applications*, *3*. doi:10.1016/j.csa.2025.100089

Thakur, G., Chouksey, P., Chopra, M., Sadotra, P., & Kumar, S. (2025, December 1). A comprehensive review on the hybrid BB84 E91 QKD protocol for enhanced security efficiency and practical hardware implementation in quantum cryptography. *Discover Computing*. Springer Science and Business Media B.V. doi:10.1007/s10791-025-09807-8

Yan, W., Zheng, X., Wen, W., Lu, L., Du, Y., Lu, Y. Q., … Ma, X. S. (2025). A measurement-device-independent quantum key distribution network using optical frequency comb. *Npj Quantum Information*, *11*(1). doi:10.1038/s41534-025-01052-7

Zapatero, V., Navarrete, Á., & Curty, M. (2025, February 1). Implementation Security in Quantum Key Distribution. *Advanced Quantum Technologies*. John Wiley and Sons Inc. doi:10.1002/qute.202300380

Zapatero, V., Wang, W., & Curty, M. (2023). A fully passive transmitter for decoy-state quantum key distribution. *Quantum Science and Technology*, *8*(2). doi:10.1088/2058-9565/acbc46

*name of corresponding author